



DEPARTMENT OF THE ARMY  
HEADQUARTERS, EASTERN REGION  
UNITED STATES ARMY CADET COMMAND  
BUILDING 1468, 328 THIRD AVENUE  
FORT KNOX, KY 40121-5117

REPLY TO  
ATTENTION OF:

ATOE-IM

16 MAY 2007

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Eastern Region Policy Letter 18 - **Security of Laptops, Portable Computer Systems and Information**

1. References:

- a. AR 25-55, 1 November 1997, Department of Army Freedom of Information Act Program.
- b. AR 25-2, 14 November 2003, Information Assurance.
- c. AR 190-51, 30 September 1993, Security of Unclassified Army Property (Sensitive and Non-sensitive).
- d. AR 380-5, 29 September, 2000, Department of The Army Information Security Program.
- e. AR 735-5, 28 February 2005.
- f. Memorandum, HQ TRADOC, ATIM-S, 31 Oct 06, Guidance on Protecting Data-At-Rest (DAR).
- g. Uniform Code of Military Justice (UCMJ), Articles 92 and 134.

2. Applicability: This policy applies to and is binding on all military and civilian personnel assigned, attached, detailed or on temporary duty with the Headquarters, Eastern Region (HQR), US Army Cadet Command.

3. Enforceability: Violations of paragraph 9 of this policy are punitive. Military personnel violating this policy may be subject to action under the UCMJ and/or adverse administrative action. Civilian employees who violate this policy may also be subject to adverse action or discipline in accordance with applicable laws and regulations.

4. Commanders, supervisors and leaders must ensure all personnel are aware of their responsibility to prevent the loss or theft of government owned or leased information technology (IT) equipment including mobile IT such as laptop computers. Laptop computers are known targets of theft because of their portability, cost and likelihood to contain sensitive

**SUBJECT: Eastern Region Policy Letter 18 - Security of Laptops, Portable Computer Systems and Information**

information. This policy provides guidance on the security of HQER laptops and portable computer systems.

5. Each individual who has responsibility for a HQER laptop computer must understand that the equipment is a sensitive item. In addition to government proprietary information, laptops often contain large quantities of Personally Identifiable Information (PII) and For Official Use Only (FOUO) data. Unauthorized access creates potential risks to HQER and Army operations ranging from disclosure of sensitive personal and operational information to intrusions and data gathering within our network. The loss of laptops causes reductions in productivity, triggers notification requirements and may subject HQER personnel to legal liability. In the wrong hands, this information may damage the reputations of HQER and the U.S. Army. My expectations include:

a. Eastern Region, Brigade and Battalion Headquarters. When not using your laptop, secure it with a cable lock, in a locked office or other secure location within your building. Proper use of cable locks is required. Commanders are responsible for evaluating this risk and vulnerabilities of loss and theft and must take all reasonable measures necessary to ensure adequate safeguards are in place for all sensitive information and equipment.

b. Laptop computers, which are not assigned to HQER personnel (due to illness or temporary absence, i.e. leave, school), will be secured in a lockable container out of plain view. Assigned laptops will be secured with cable locks.

c. The issuance of laptop cable locks, instructions and required key control requirements will be in conjunction with or in the same manner as laptops currently issued. The commander will establish key control for all his assigned laptop security cables.

d. All laptop computers will have approved encryption software installed to protect against information being compromised.

6. Lost or stolen IT equipment, including laptops, must immediately be reported by the chain of command as a serious incident. Any adverse administrative action, including financial liability investigations or punitive action administered against any personnel violating this policy will be reported to the chain of command and the Staff Judge Advocate as a follow-up to the original serious incident report.

7. Liability for the loss or theft of laptop computers shall be evaluated in accordance with this policy and AR 735-5. Failure to follow this policy or other guidance on laptop security will constitute negligence and subject the violator to personal liability.

8. Keys for cable locks will be included in unit key control procedures and monthly and semi-annual inventories will be conducted. Inventories of laptop computers will be conducted IAW 10% cyclic inventory procedures.

**SUBJECT: Eastern Region Policy Letter 18 - Security of Laptops, Portable Computer Systems and Information**

9. The following procedures must be followed:

a. When traveling with a laptop outside the regular place of duty:

(1) HQER/responsible personnel will not leave a laptop unattended in a government owned vehicle or privately owned vehicle. The prohibition applies even if the vehicle is locked, the computer is in the trunk or secured by an approved locking device.

(2) HQER/responsible personnel will carry the laptop on their person or otherwise maintain positive visual or physical control of the laptop when traveling by airplane or train. If the computer carrying case is too large to be carried on an airplane, HQER/responsible personnel are required to take the computer out of the case and hand carry it on the airplane.

(3) HQER/responsible personnel will not leave a laptop unattended in an unsecured hotel room.


b. HQER/responsible personnel will not leave a laptop unattended in an unsecured personal residence.

c. HQER/responsible personnel will not leave a laptop unattended unless it is secured with a cable lock or other approved locking device. Unassigned laptop computers will be secured in a locked closet, locked cabinet or locked filing cabinet.

10. Although portions of this policy are punitive, commanders are reminded to consider their full range of options for addressing misconduct and to dispose of the case at the lowest appropriate level having authority consistent with the gravity of the case.

11. This policy will remain in effect until superseded or rescinded.

"Train to Lead--We Commission."

  
ROY C. WAGGONER III  
COL, IN  
Commanding

DISTRIBUTION:

A